FIG. 1

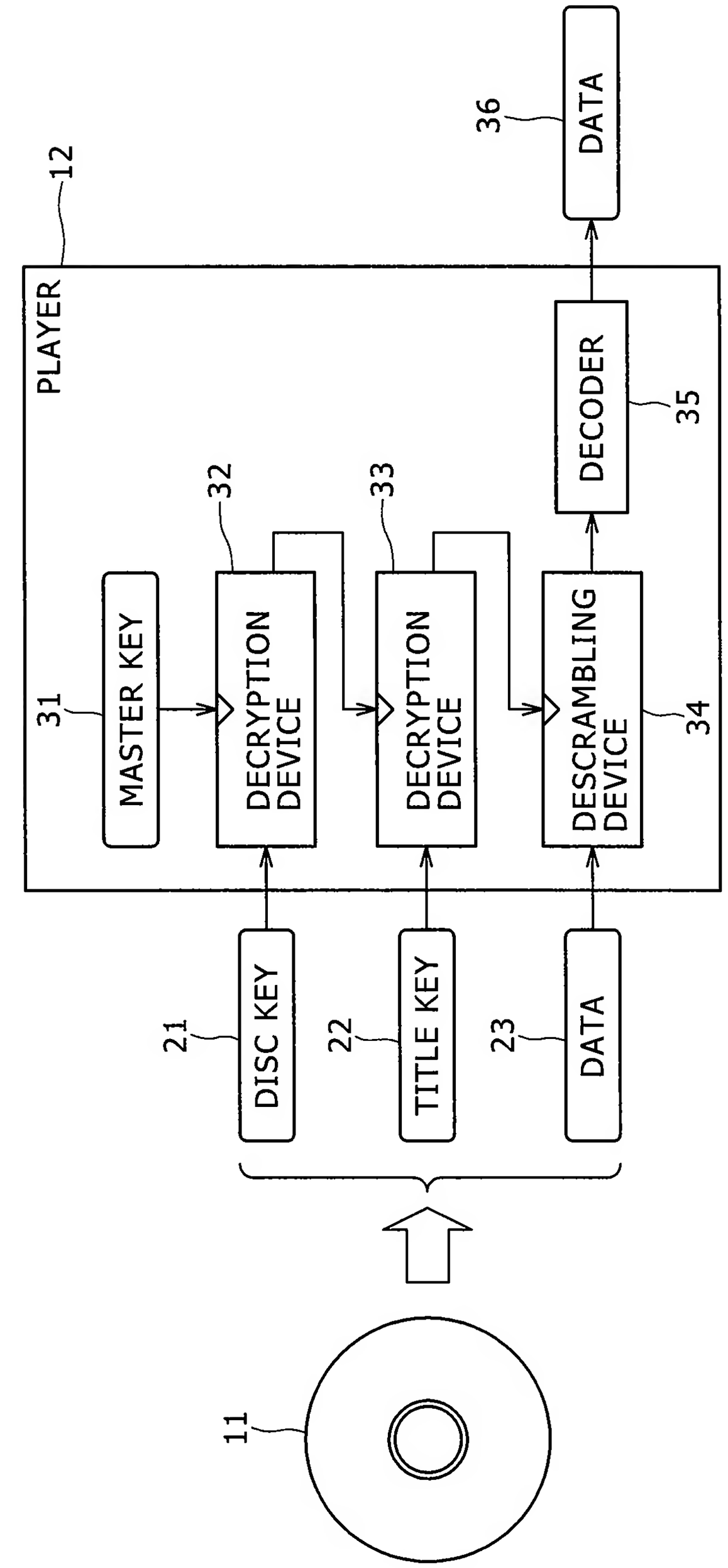

11
DISC
21
DISC KEY
22
TITLE KEY
23
DATA
PLAYER
31
MASTER KEY
32
DECRYPTION DEVICE
33
DECRYPTION DEVICE
34
DESCRAMBLING DEVICE
35
DECODER
36
DATA
12

FIG. 2

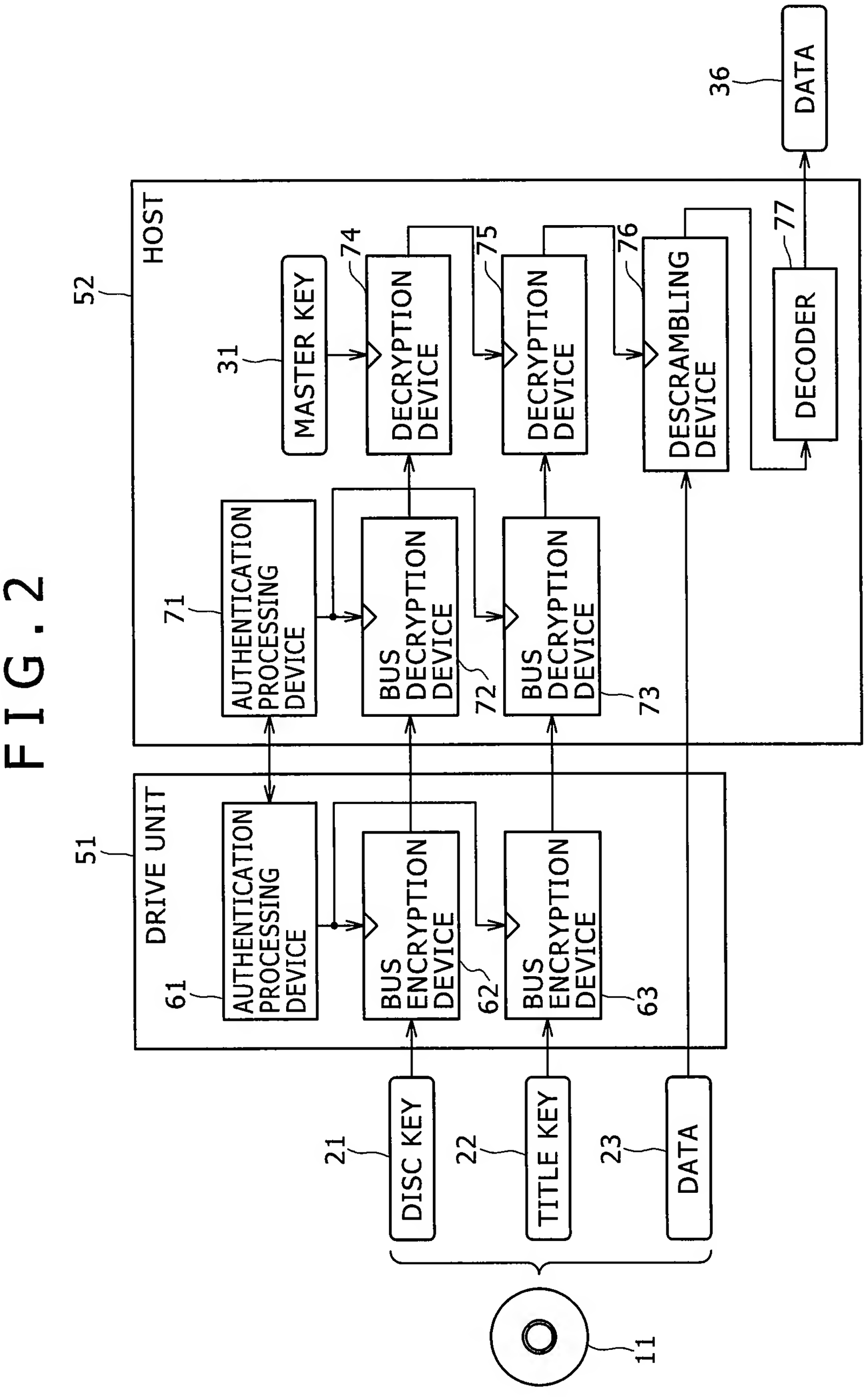

11
DISC KEY
21
TITLE KEY
22
DATA
23
DRIVE UNIT
51
AUTHENTICATION PROCESSING DEVICE
61
BUS ENCRYPTION DEVICE
62
BUS ENCRYPTION DEVICE
63
HOST
52
MASTER KEY
31
AUTHENTICATION PROCESSING DEVICE
71
BUS DECRYPTION DEVICE
72
BUS DECRYPTION DEVICE
73
DECRYPTION DEVICE
74
DECRYPTION DEVICE
75
DESCRAMBLING DEVICE
76
DECODER
77
DATA
36

FIG.3

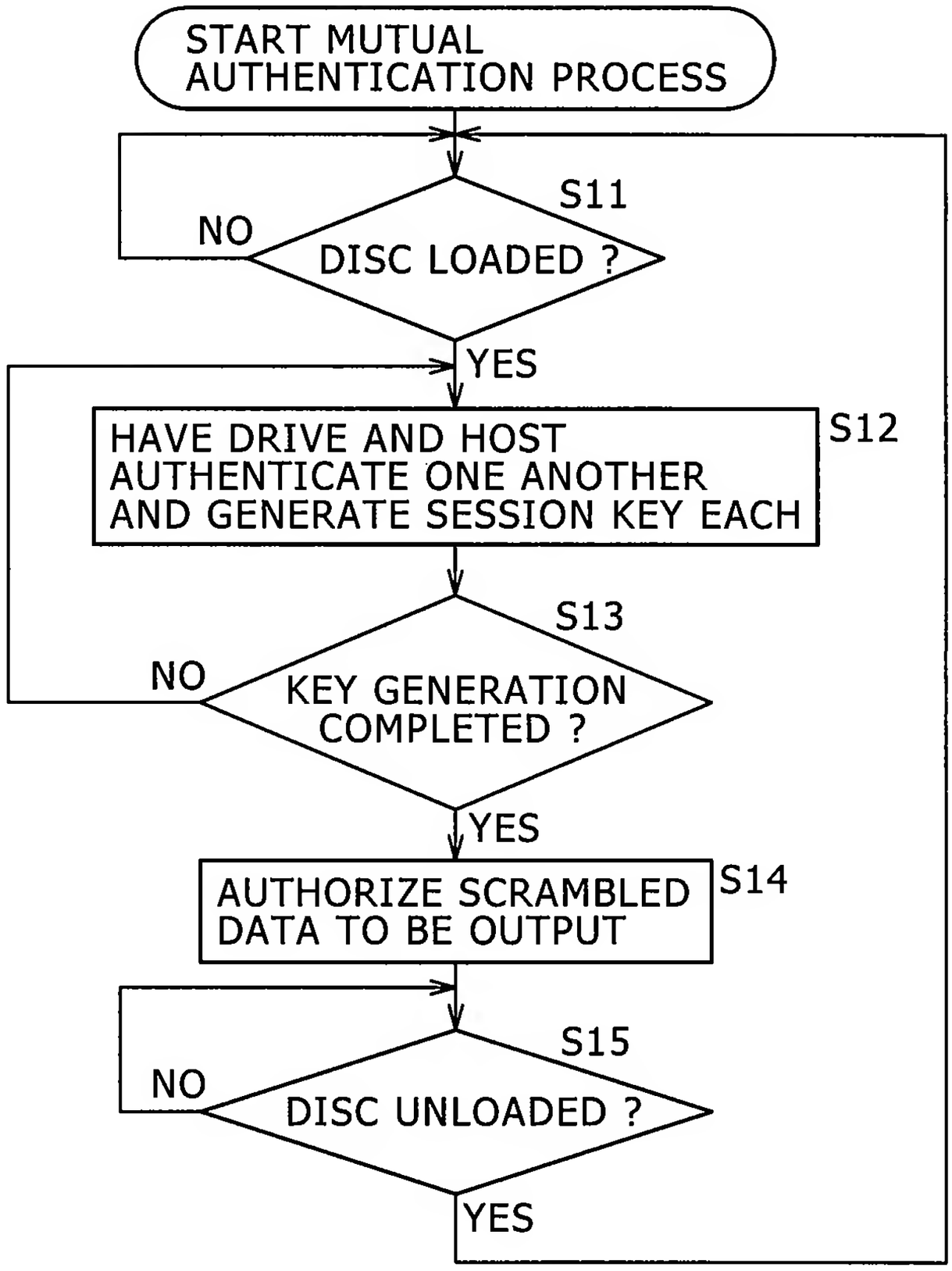

START MUTUAL AUTHENTICATION PROCESS
S11
NO
DISC LOADED ?
YES
HAVE DRIVE AND HOST AUTHENTICATE ONE ANOTHER AND GENERATE SESSION KEY EACH
S12
S13
NO
KEY GENERATION COMPLETED ?
YES
AUTHORIZE SCRAMBLED DATA TO BE OUTPUT
S14
S15
NO
DISC UNLOADED ?
YES

FIG.4

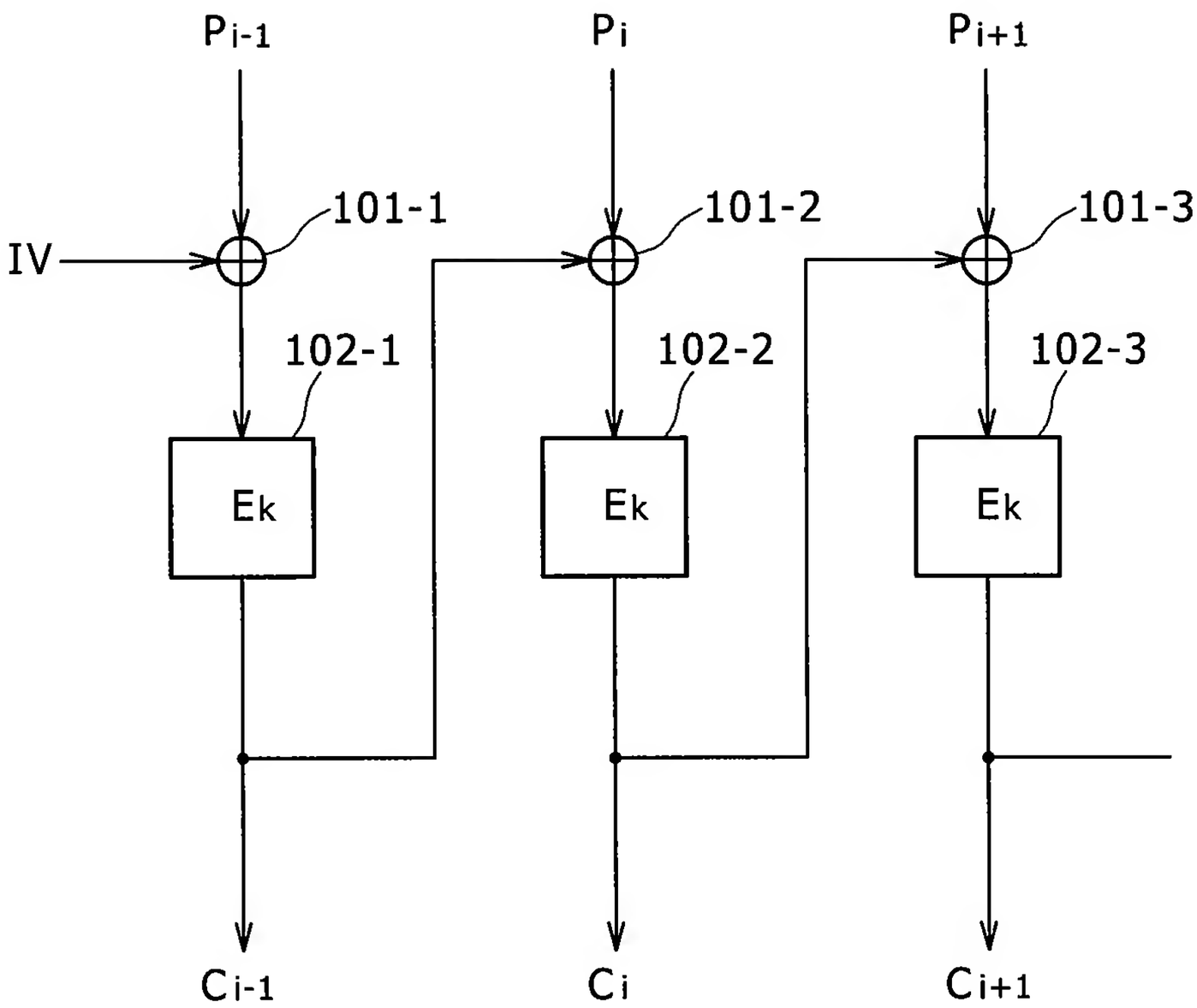


FIG. 5

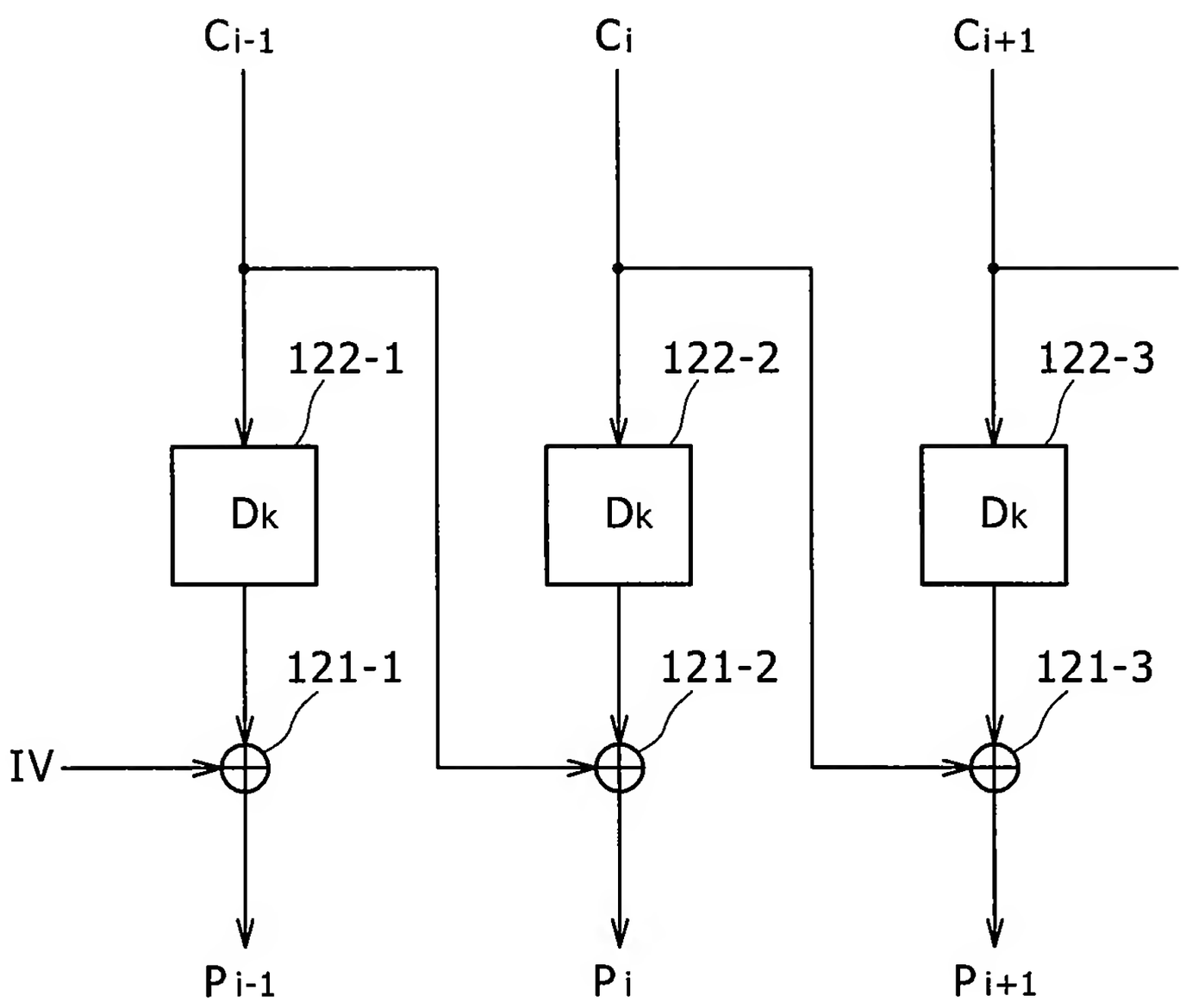


FIG. 6

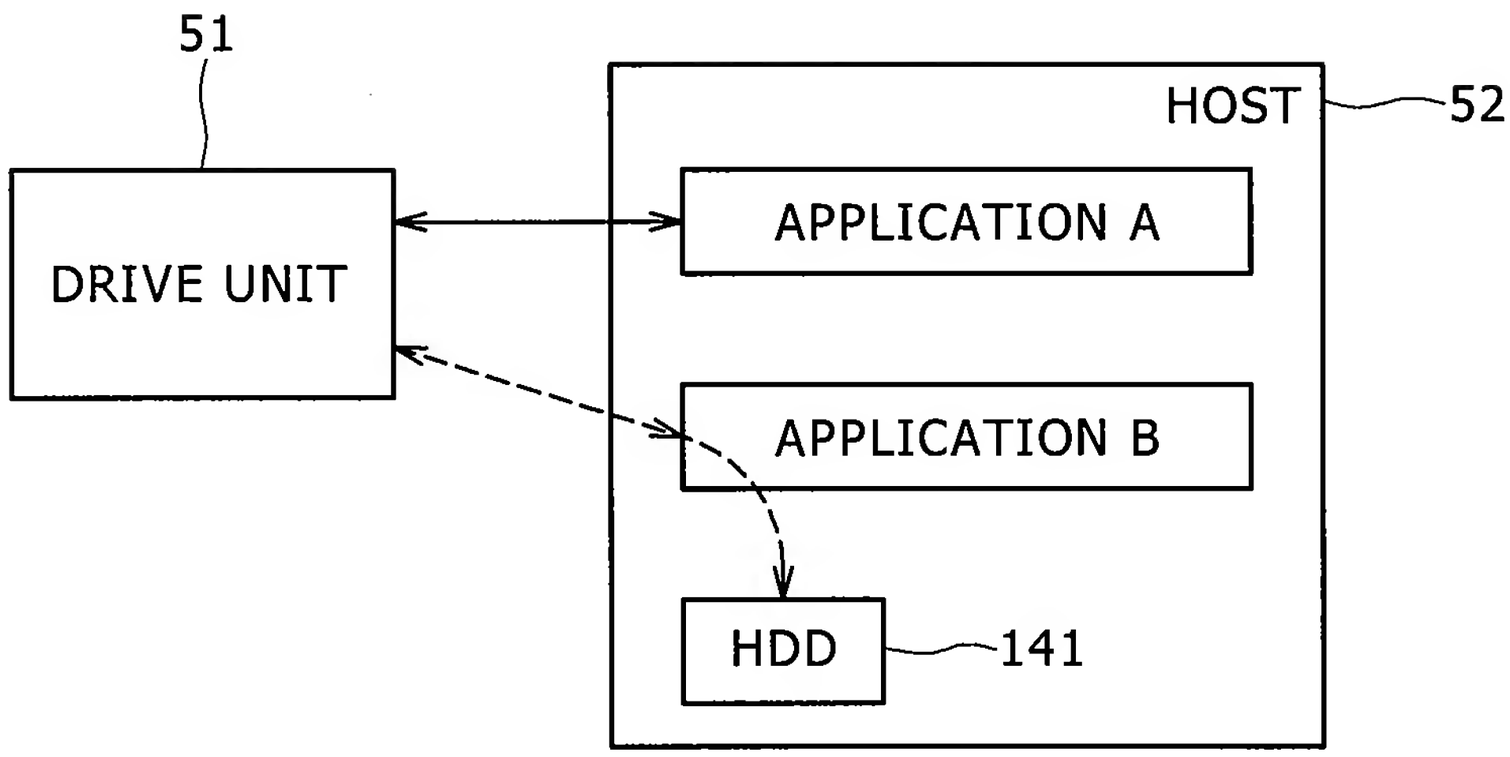


FIG. 7

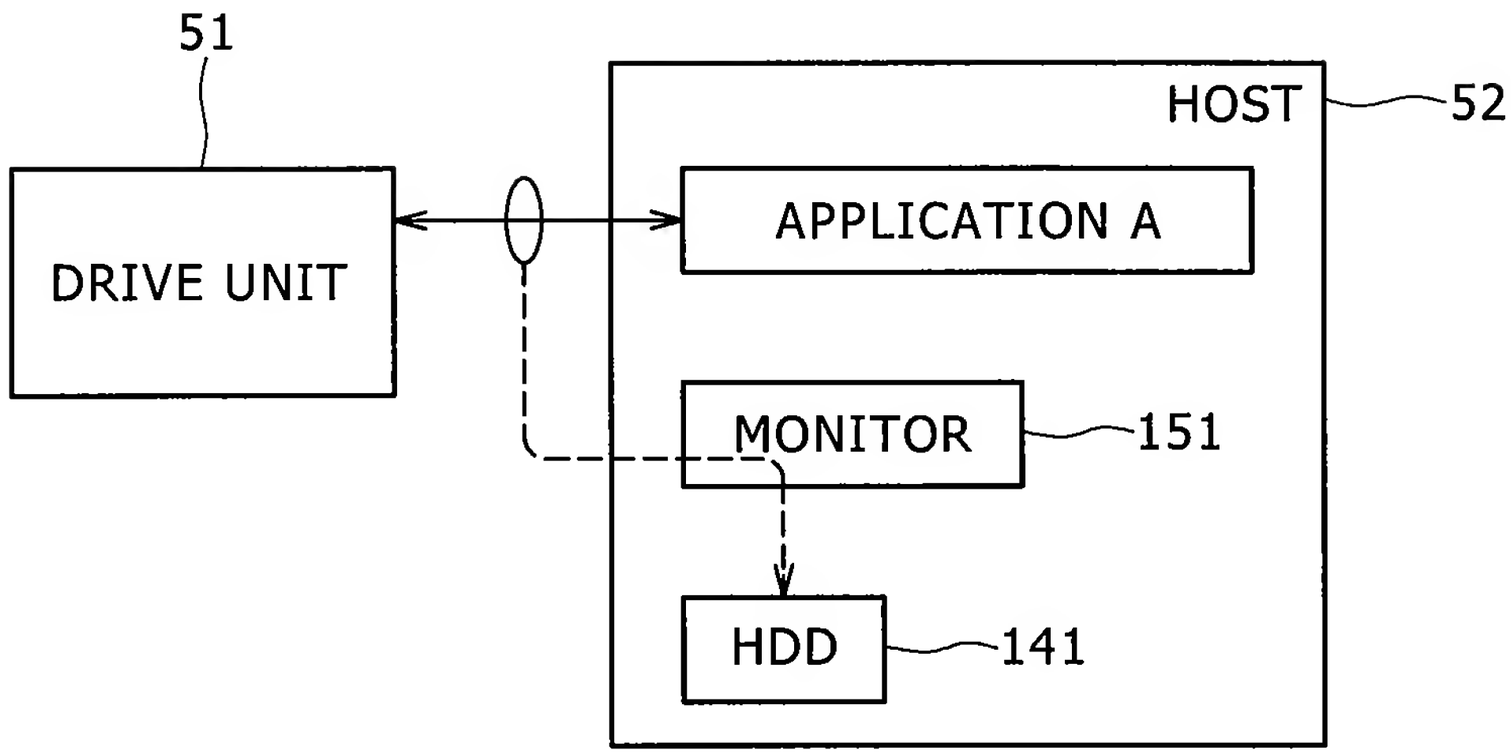


FIG. 8

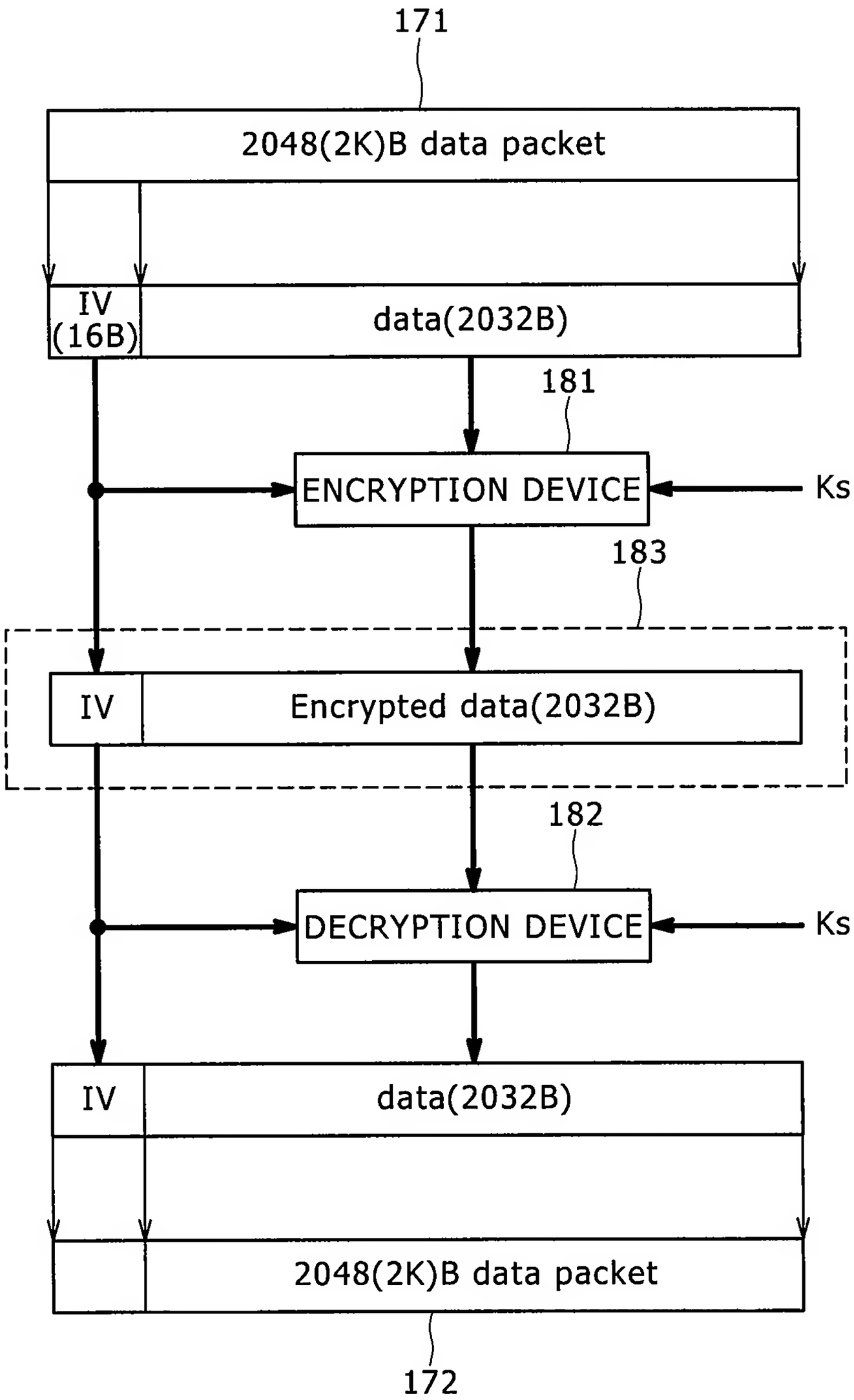

171
2048(2K)B data packet
IV (16B)
data(2032B)
181
ENCRYPTION DEVICE
Ks
183
IV
Encrypted data(2032B)
182
DECRYPTION DEVICE
Ks
IV
data(2032B)
2048(2K)B data packet
172

FIG. 9

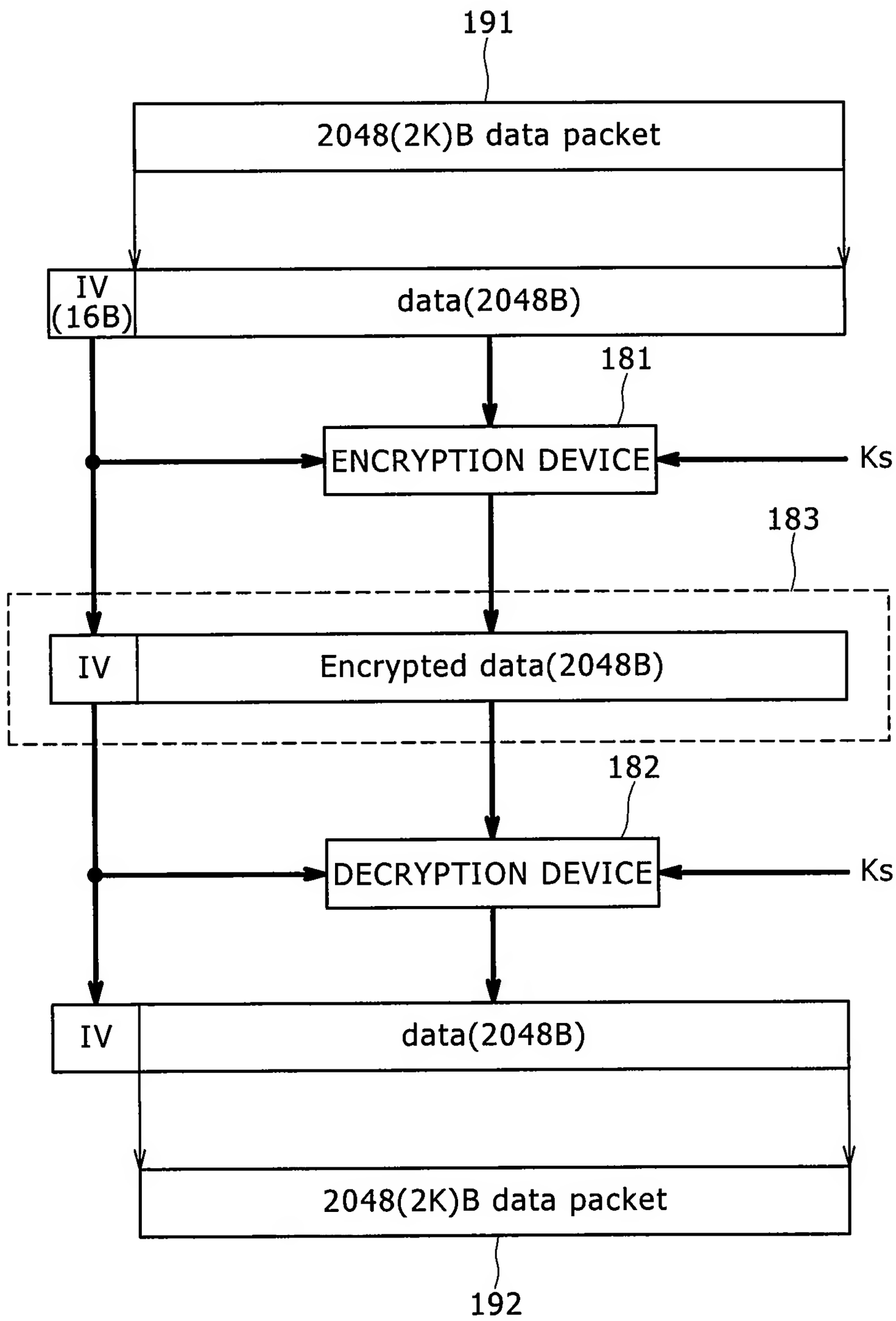

191
2048(2K)B data packet
IV (16B)
data(2048B)
181
ENCRYPTION DEVICE
Ks
183
IV
Encrypted data(2048B)
182
DECRYPTION DEVICE
Ks
IV
data(2048B)
2048(2K)B data packet
192

FIG. 10

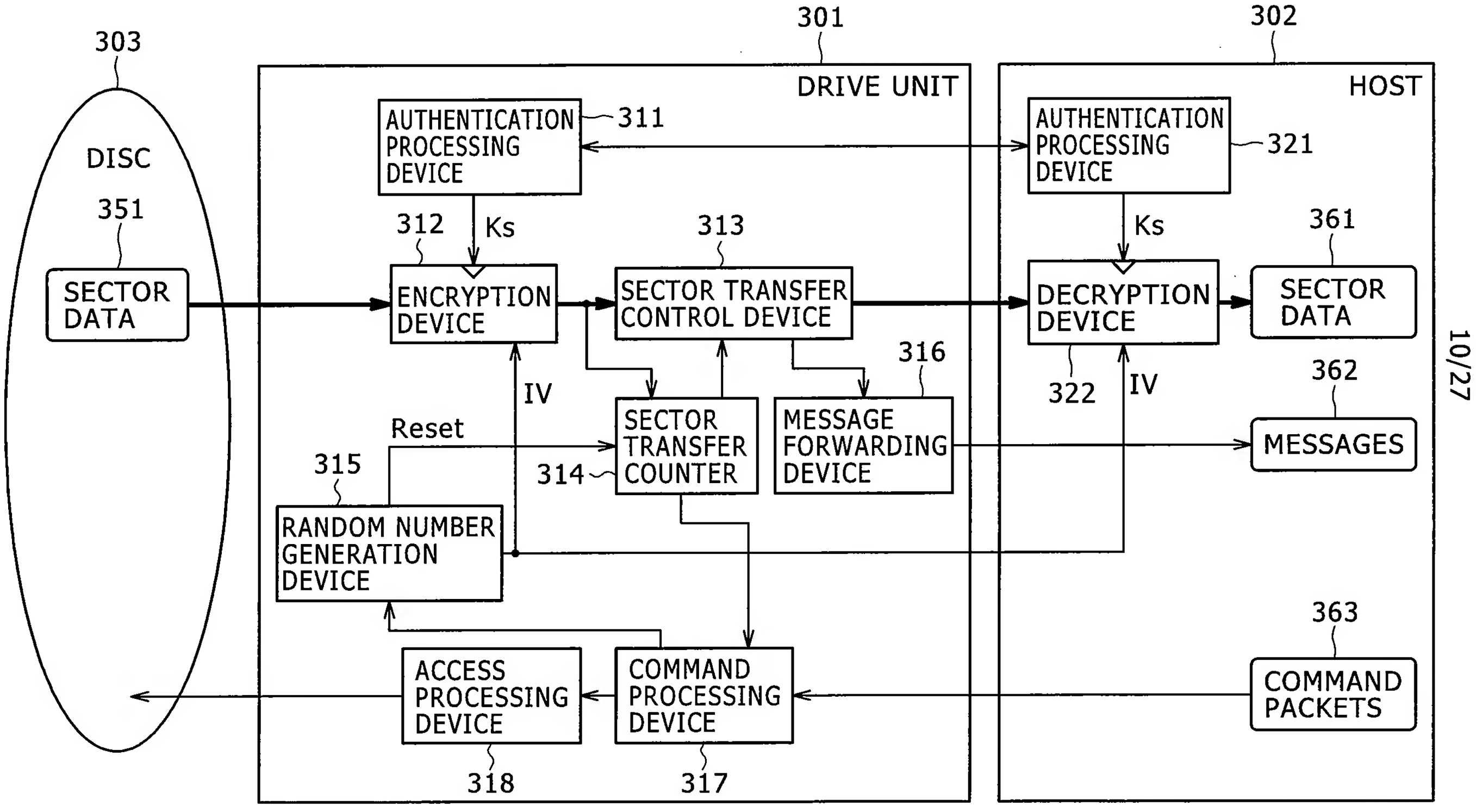

303
DISC
351
SECTOR DATA
301
DRIVE UNIT
AUTHENTICATION PROCESSING DEVICE
311
312
Ks
ENCRYPTION DEVICE
313
SECTOR TRANSFER CONTROL DEVICE
316
IV
SECTOR TRANSFER COUNTER
314
MESSAGE FORWARDING DEVICE
Reset
315
RANDOM NUMBER GENERATION DEVICE
ACCESS PROCESSING DEVICE
318
COMMAND PROCESSING DEVICE
317
302
HOST
AUTHENTICATION PROCESSING DEVICE
321
Ks
DECRYPTION DEVICE
322
IV
361
SECTOR DATA
362
MESSAGES
363
COMMAND PACKETS

FIG. 11

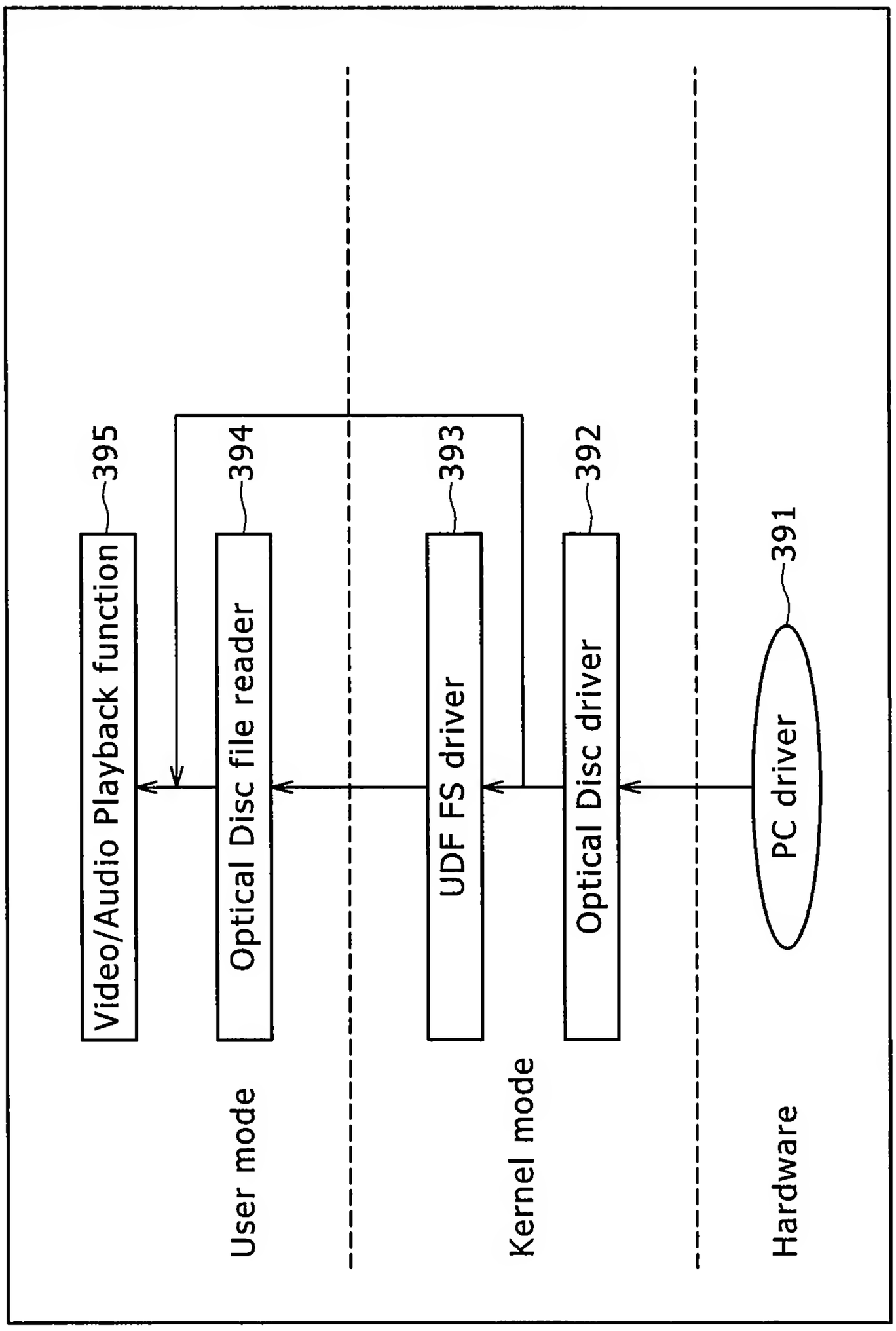

Video/Audio Playback function
395
Optical Disc file reader
394
UDF FS driver
393
Optical Disc driver
392
PC driver
391
User mode
Kernel mode
Hardware

FIG. 12

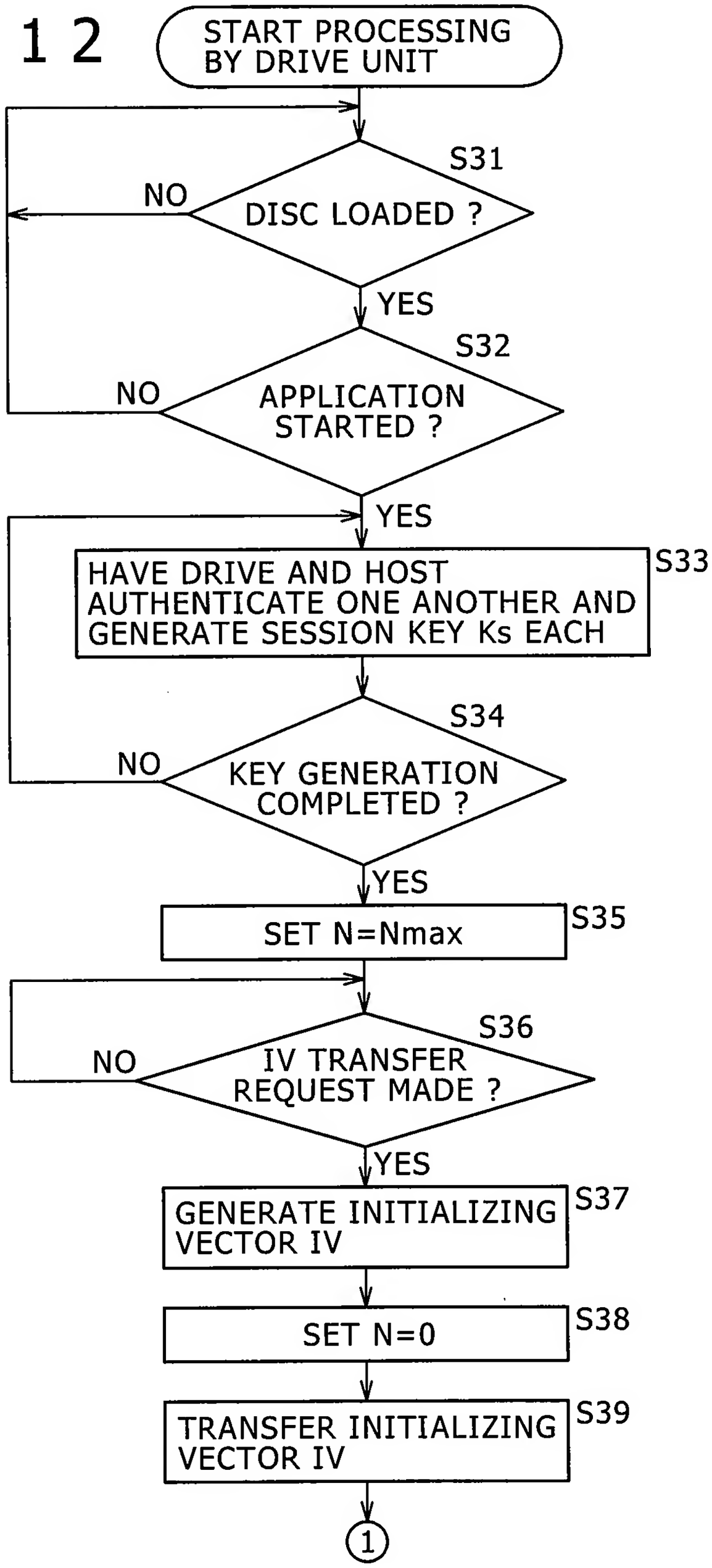

START PROCESSING BY DRIVE UNIT
S31
DISC LOADED ?
NO
YES
S32
APPLICATION STARTED ?
NO
YES
S33
HAVE DRIVE AND HOST AUTHENTICATE ONE ANOTHER AND GENERATE SESSION KEY Ks EACH
S34
KEY GENERATION COMPLETED ?
NO
YES
S35
SET N=Nmax
S36
IV TRANSFER REQUEST MADE ?
NO
YES
S37
GENERATE INITIALIZING VECTOR IV
S38
SET N=0
S39
TRANSFER INITIALIZING VECTOR IV
1

FIG. 13

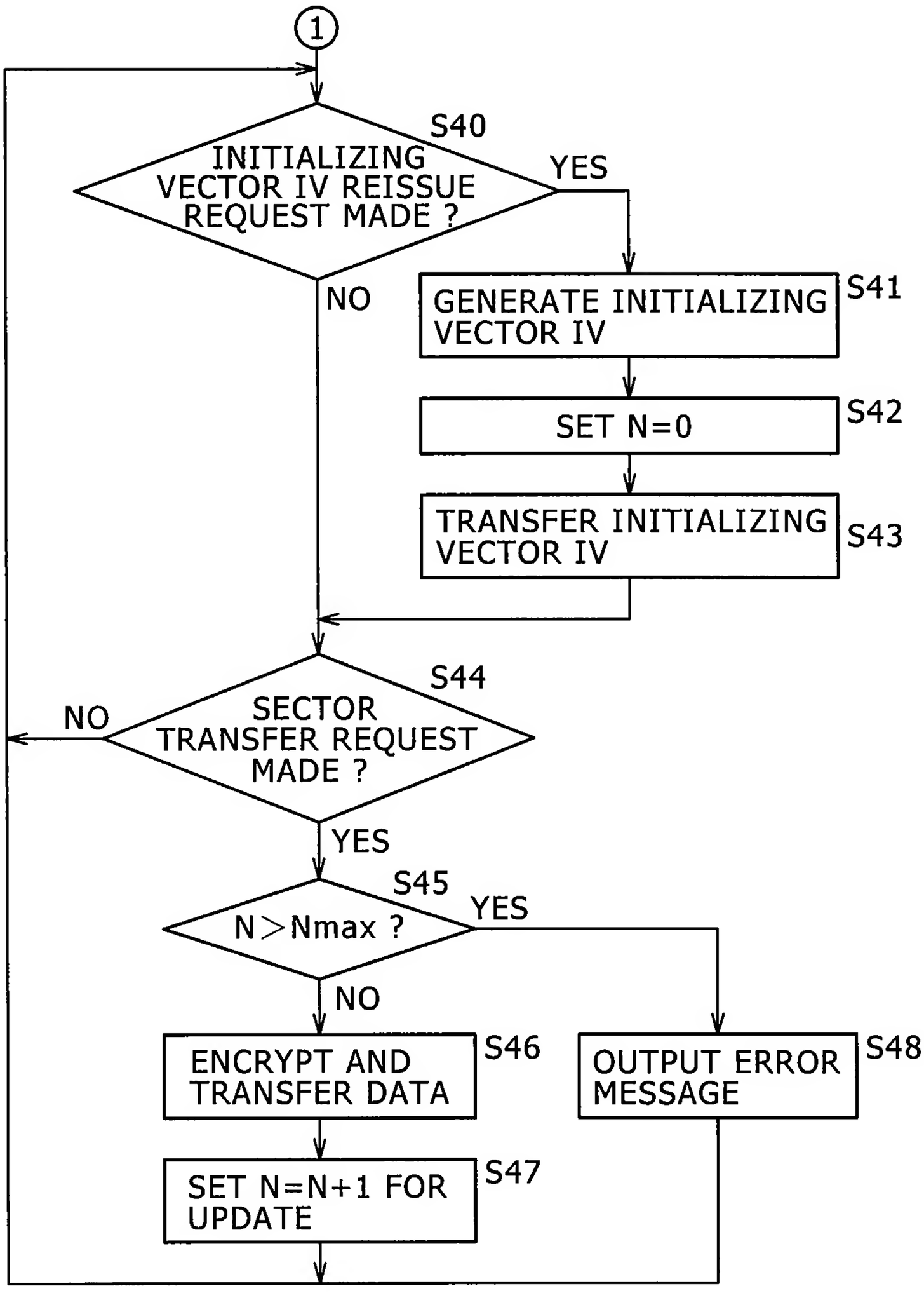

1
S40
INITIALIZING VECTOR IV REISSUE REQUEST MADE ?
YES
NO
S41
GENERATE INITIALIZING VECTOR IV
S42
SET N=0
S43
TRANSFER INITIALIZING VECTOR IV
S44
SECTOR TRANSFER REQUEST MADE ?
NO
YES
S45
N>Nmax ?
YES
NO
S46
ENCRYPT AND TRANSFER DATA
S47
SET N=N+1 FOR UPDATE
S48
OUTPUT ERROR MESSAGE

FIG.14

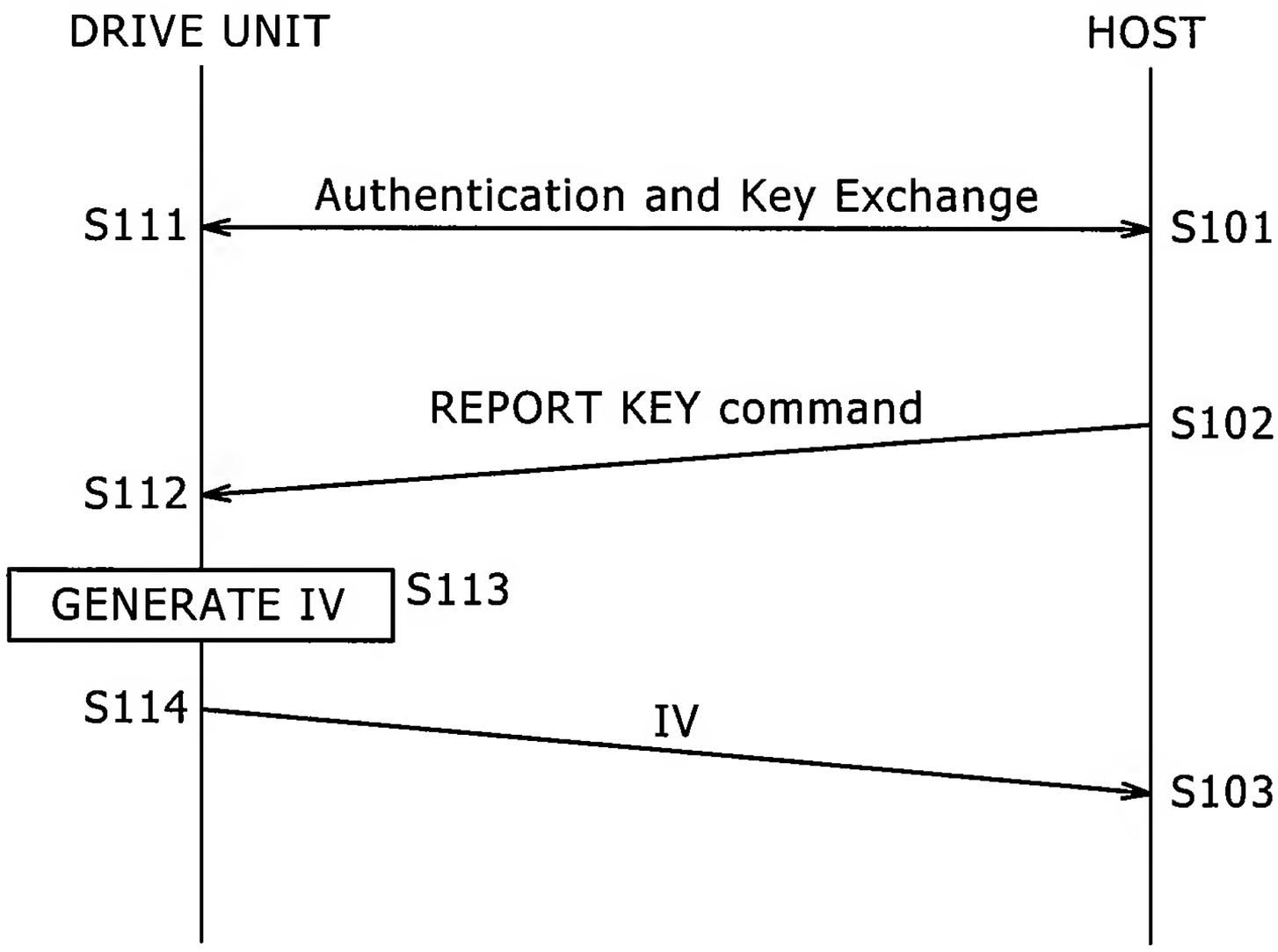

DRIVE UNIT
HOST
S111
Authentication and Key Exchange
S101
REPORT KEY command
S102
S112
GENERATE IV
S113
S114
IV
S103

FIG. 15

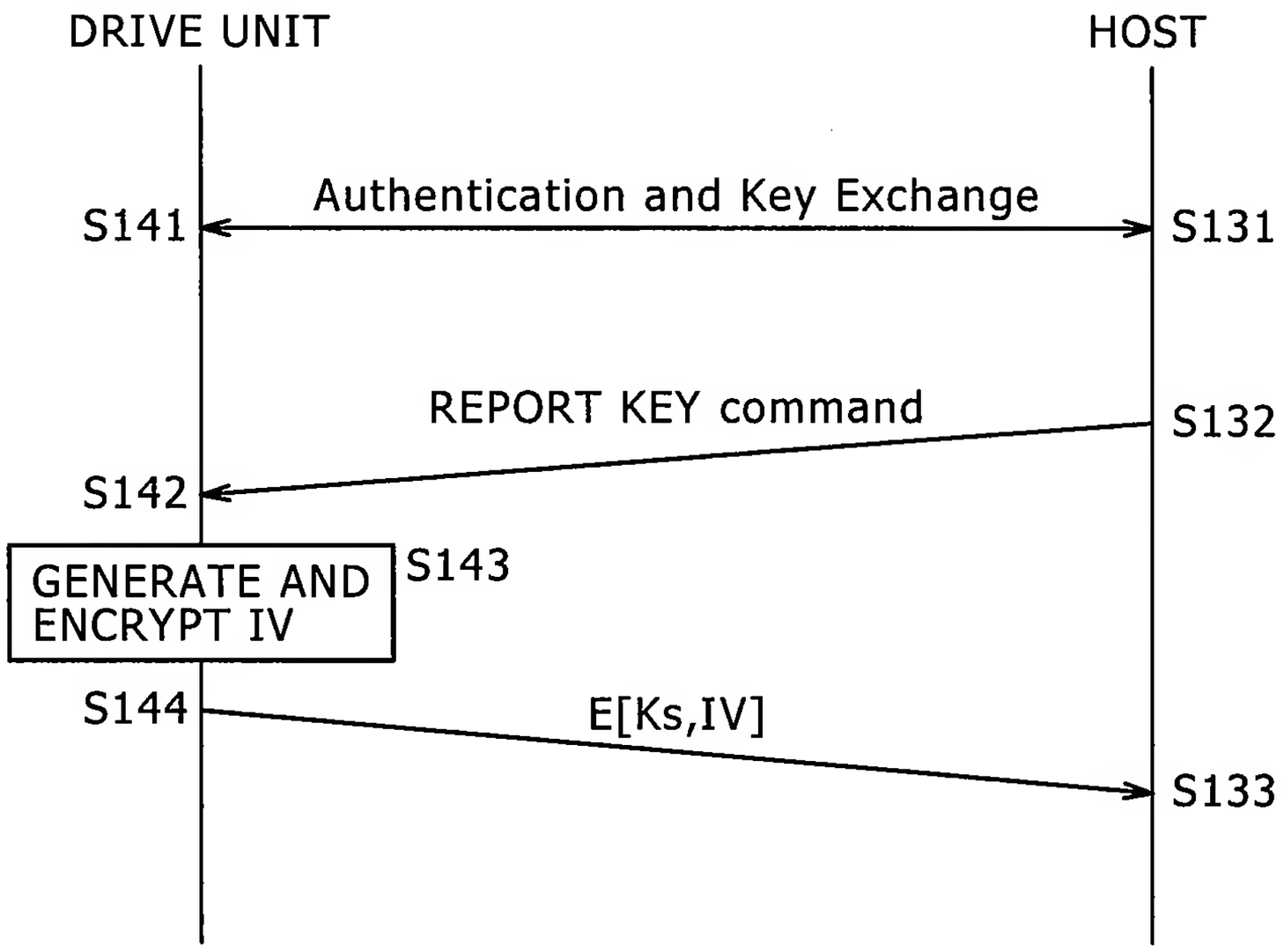

DRIVE UNIT
HOST
S141
Authentication and Key Exchange
S131
REPORT KEY command
S132
S142
GENERATE AND ENCRYPT IV
S143
S144
E[Ks,IV]
S133

FIG. 16

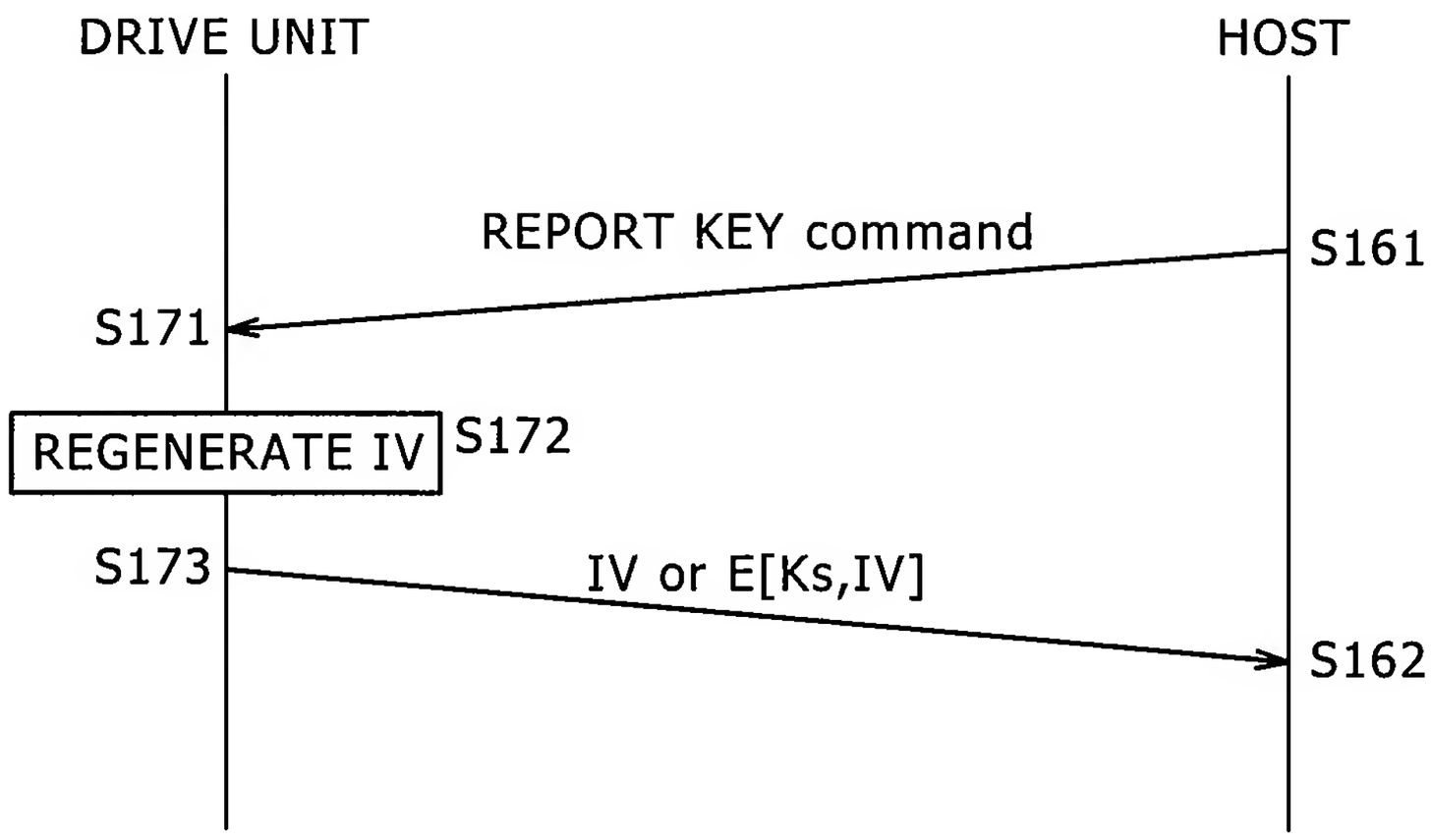

DRIVE UNIT
HOST
REPORT KEY command
S161
S171
REGENERATE IV
S172
S173
IV or E[Ks,IV]
S162

FIG. 17

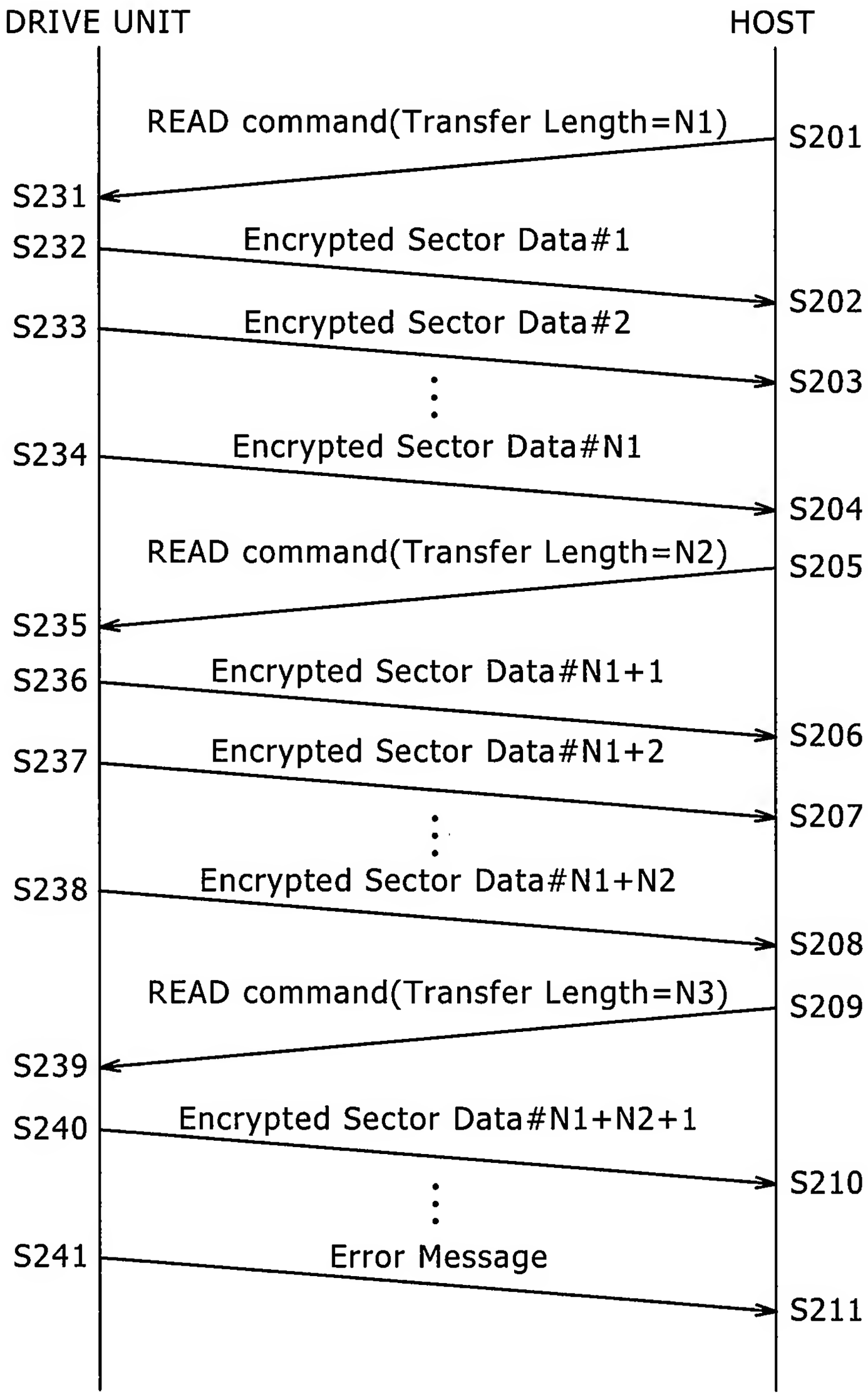
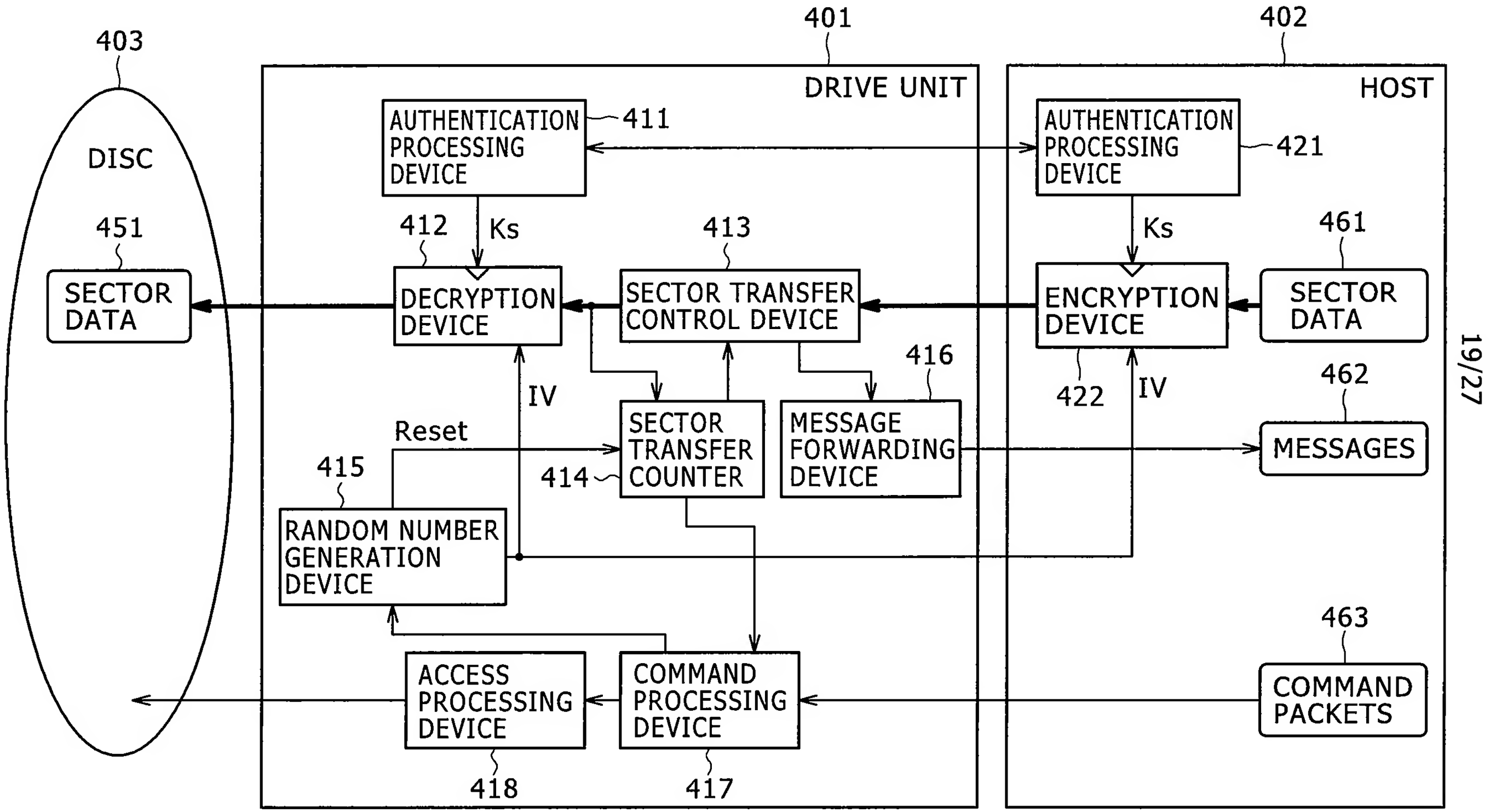

DRIVE UNIT
HOST
READ command(Transfer Length=N1)
S201
S231
S232
Encrypted Sector Data#1
S202
S233
Encrypted Sector Data#2
S203
S234
Encrypted Sector Data#N1
S204
READ command(Transfer Length=N2)
S205
S235
S236
Encrypted Sector Data#N1+1
S206
S237
Encrypted Sector Data#N1+2
S207
S238
Encrypted Sector Data#N1+N2
S208
READ command(Transfer Length=N3)
S209
S239
S240
Encrypted Sector Data#N1+N2+1
S210
S241
Error Message
S211

FIG.18

363

Bit / Byte	7	6	5	4	3	2	1	0
0	Operation Code							
1	LUN(Obsolete)			DPO(0)	FUA	Reserved	RelAdr	
2	(MSB)							
3								
4								
5								(LSB)
6	(MSB)							
7								
8								
9								(LSB)
10	Reserved							
11	Reserved						NACA	Flag	Link

FIG. 19



S05P0372

FIG.20

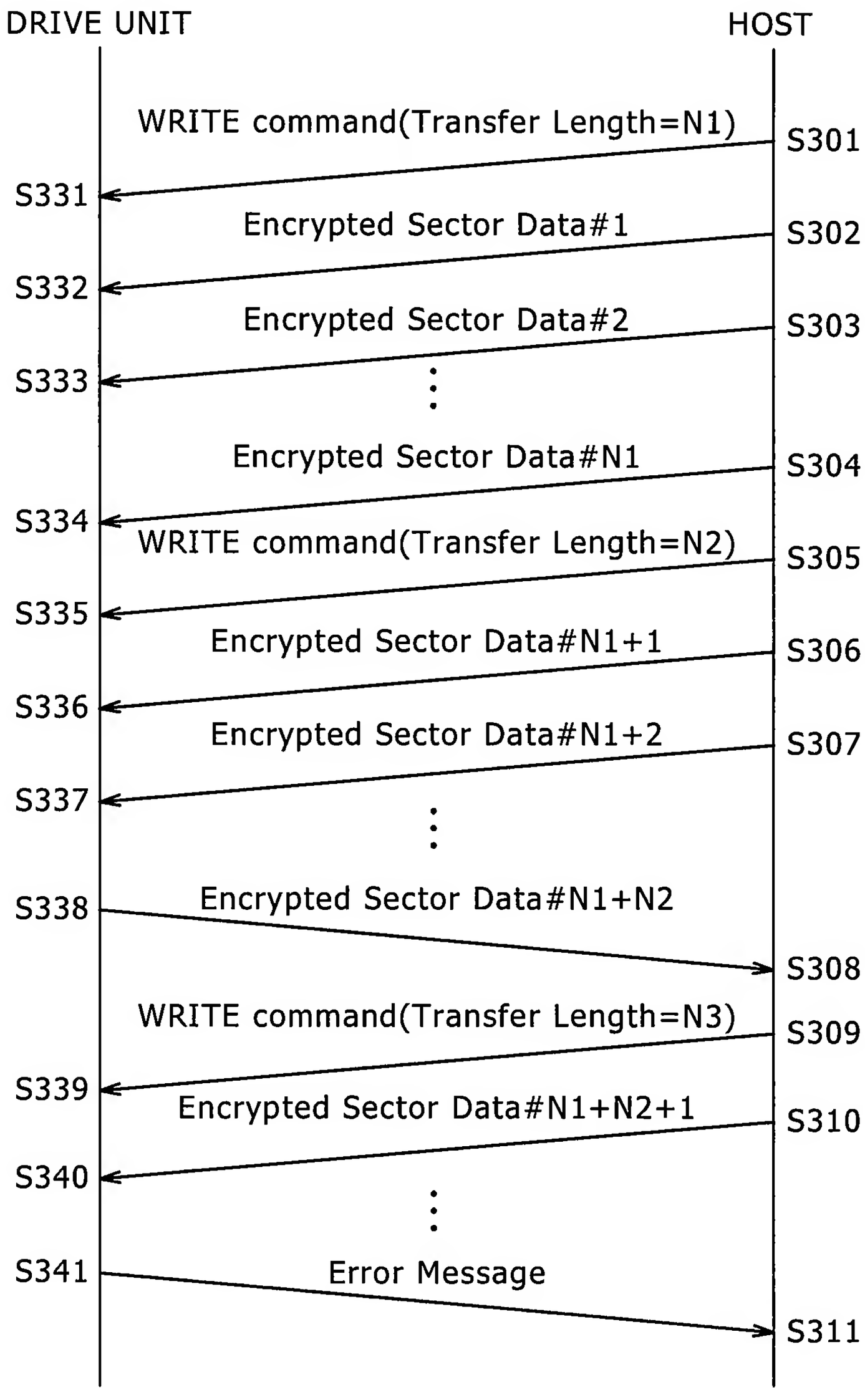

DRIVE UNIT
HOST
WRITE command(Transfer Length=N1)
S301
S331
Encrypted Sector Data#1
S302
S332
Encrypted Sector Data#2
S303
S333
Encrypted Sector Data#N1
S304
S334
WRITE command(Transfer Length=N2)
S305
S335
Encrypted Sector Data#N1+1
S306
S336
Encrypted Sector Data#N1+2
S307
S337
Encrypted Sector Data#N1+N2
S338
S308
WRITE command(Transfer Length=N3)
S309
S339
Encrypted Sector Data#N1+N2+1
S310
S340
Error Message
S341
S311

FIG. 21

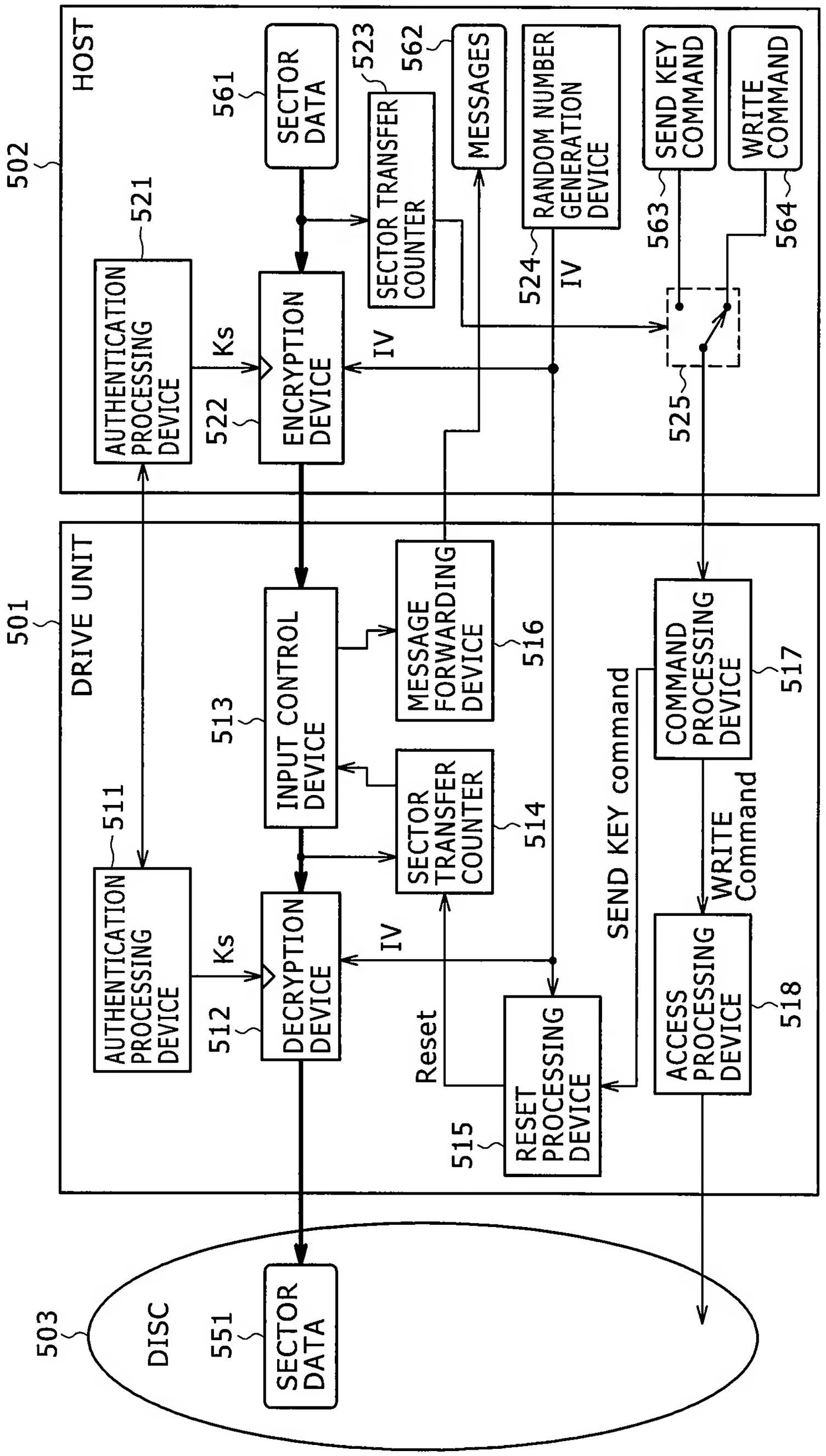

HOST
502
SECTOR DATA
561
SECTOR TRANSFER COUNTER
523
MESSAGES
562
RANDOM NUMBER GENERATION DEVICE
524
IV
SEND KEY COMMAND
563
WRITE COMMAND
564
AUTHENTICATION PROCESSING DEVICE
521
Ks
ENCRYPTION DEVICE
522
IV
525
DRIVE UNIT
501
INPUT CONTROL DEVICE
513
MESSAGE FORWARDING DEVICE
516
SECTOR TRANSFER COUNTER
514
AUTHENTICATION PROCESSING DEVICE
511
Ks
DECRYPTION DEVICE
512
IV
Reset
RESET PROCESSING DEVICE
515
SEND KEY command
COMMAND PROCESSING DEVICE
517
WRITE Command
ACCESS PROCESSING DEVICE
518
DISC
503
SECTOR DATA
551

FIG.22

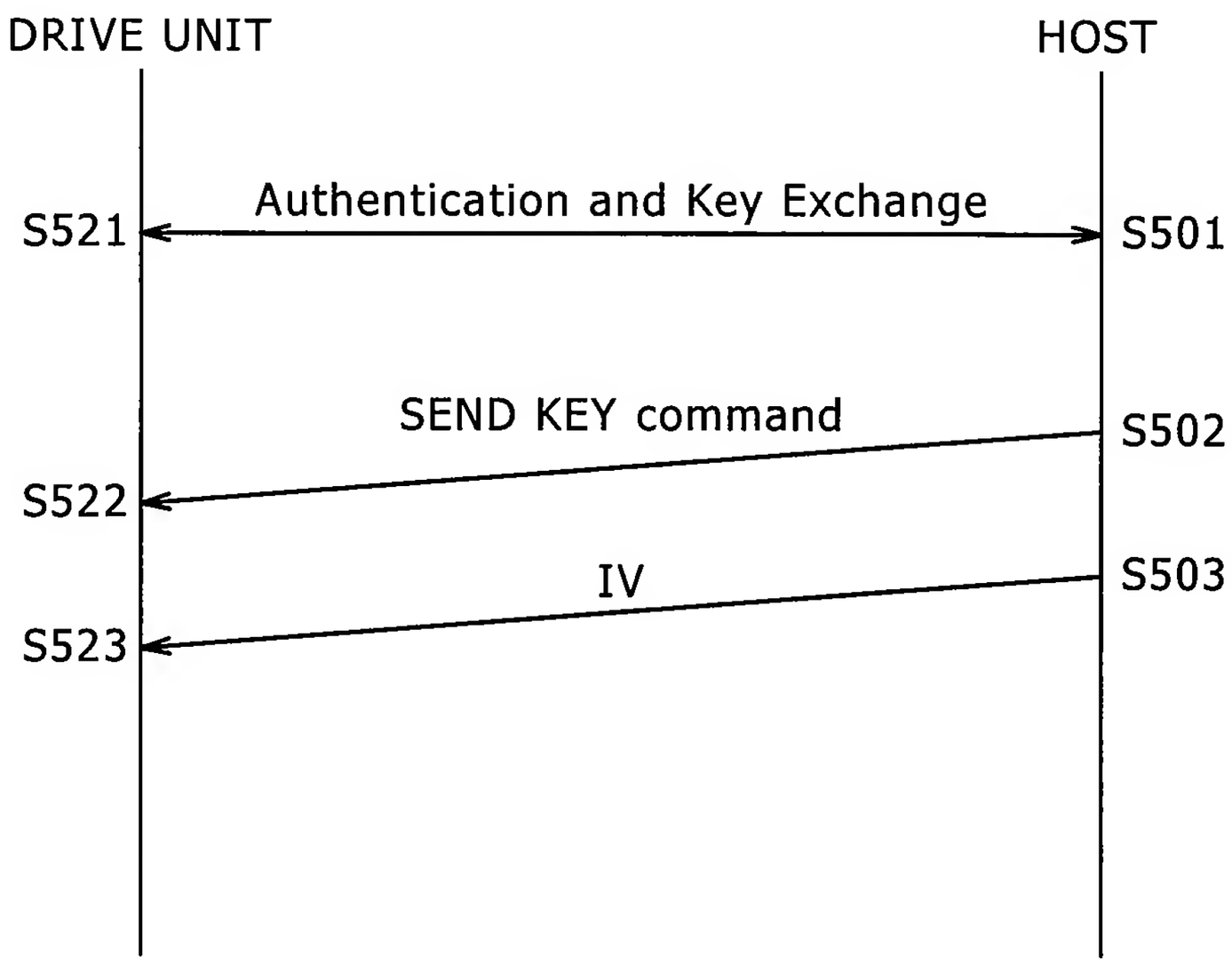

DRIVE UNIT
HOST
Authentication and Key Exchange
S521
S501
SEND KEY command
S502
S522
IV
S503
S523

FIG.23

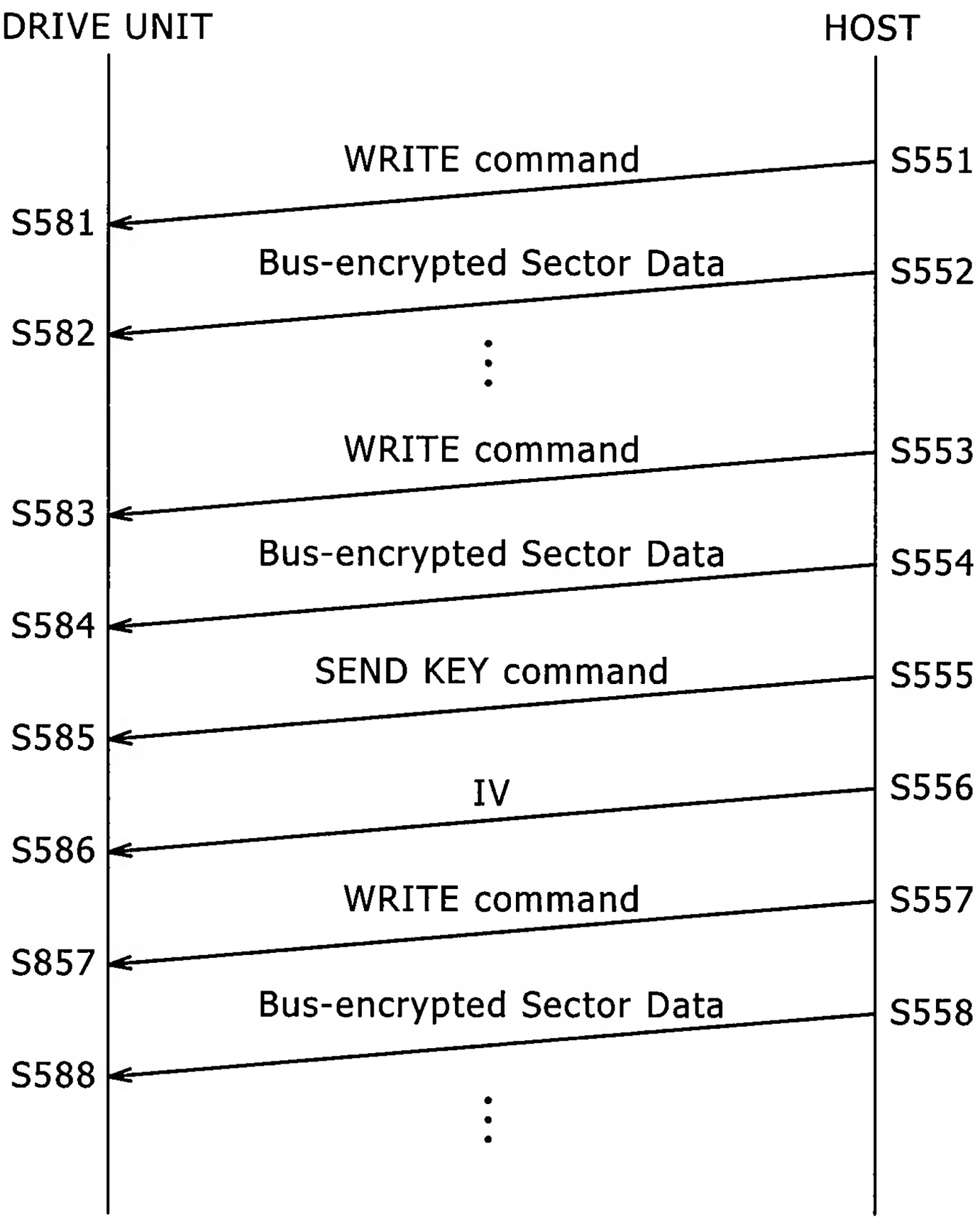

DRIVE UNIT
HOST
WRITE command
S551
S581
Bus-encrypted Sector Data
S552
S582
WRITE command
S553
S583
Bus-encrypted Sector Data
S554
S584
SEND KEY command
S555
S585
IV
S556
S586
WRITE command
S557
S857
Bus-encrypted Sector Data
S558
S588

FIG. 24

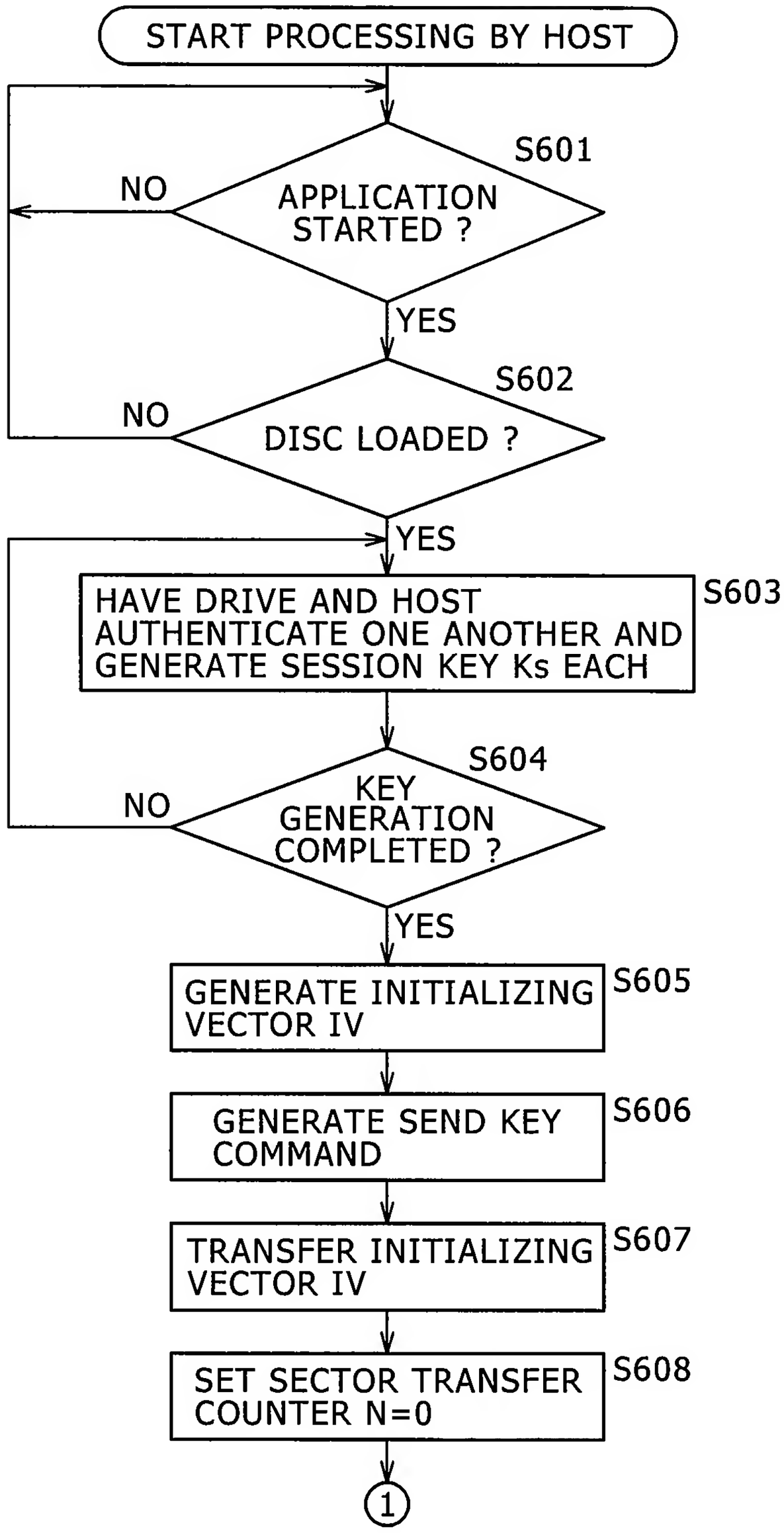

START PROCESSING BY HOST
S601
APPLICATION STARTED ?
NO
YES
S602
DISC LOADED ?
NO
YES
S603
HAVE DRIVE AND HOST AUTHENTICATE ONE ANOTHER AND GENERATE SESSION KEY Ks EACH
S604
KEY GENERATION COMPLETED ?
NO
YES
S605
GENERATE INITIALIZING VECTOR IV
S606
GENERATE SEND KEY COMMAND
S607
TRANSFER INITIALIZING VECTOR IV
S608
SET SECTOR TRANSFER COUNTER N=0
1

FIG.25

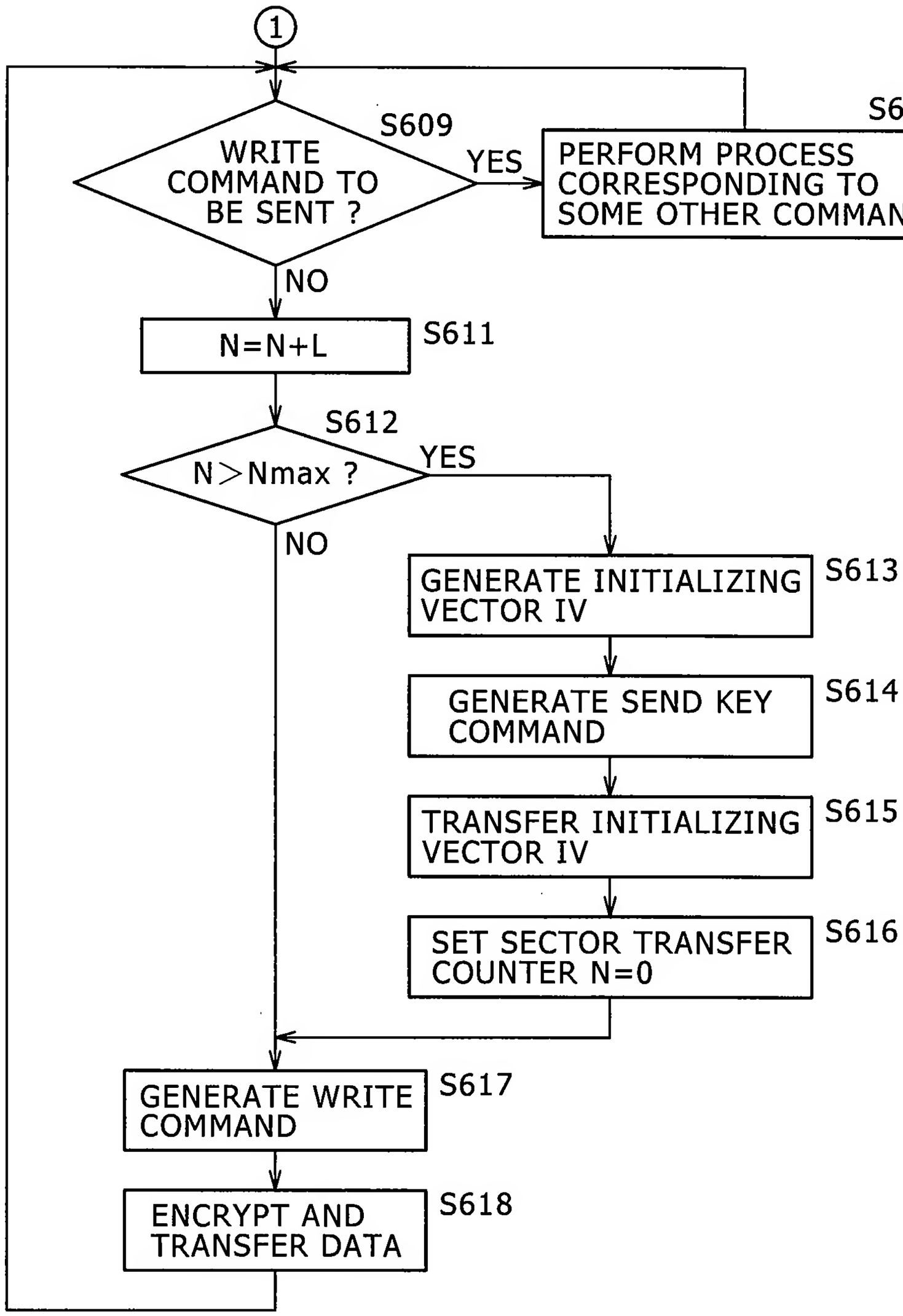

1
S609
WRITE COMMAND TO BE SENT ?
YES
S610
PERFORM PROCESS CORRESPONDING TO SOME OTHER COMMAND
NO
N=N+L
S611
S612
N>Nmax ?
YES
NO
GENERATE INITIALIZING VECTOR IV
S613
GENERATE SEND KEY COMMAND
S614
TRANSFER INITIALIZING VECTOR IV
S615
SET SECTOR TRANSFER COUNTER N=0
S616
GENERATE WRITE COMMAND
S617
ENCRYPT AND TRANSFER DATA
S618

FIG.26

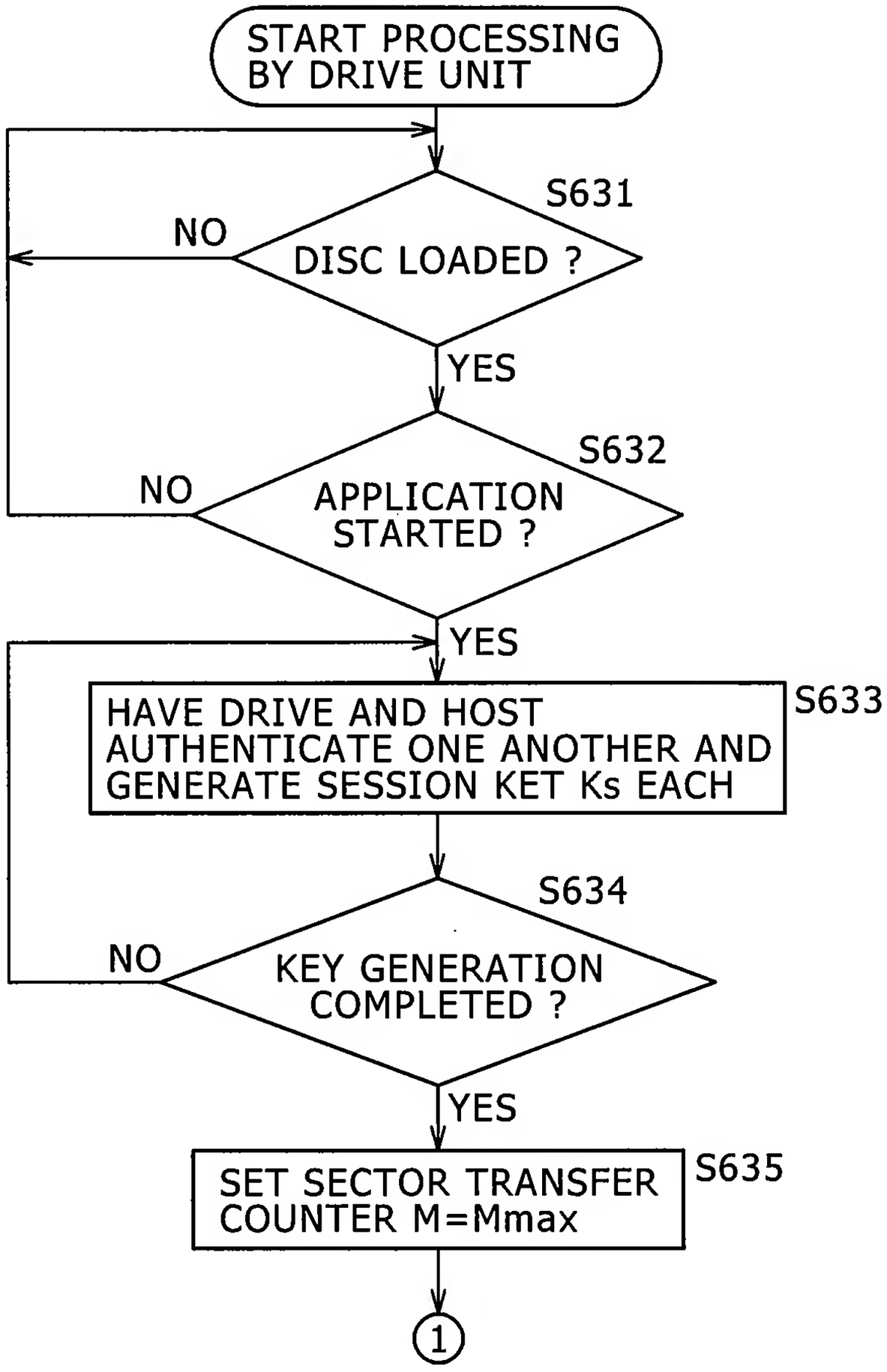
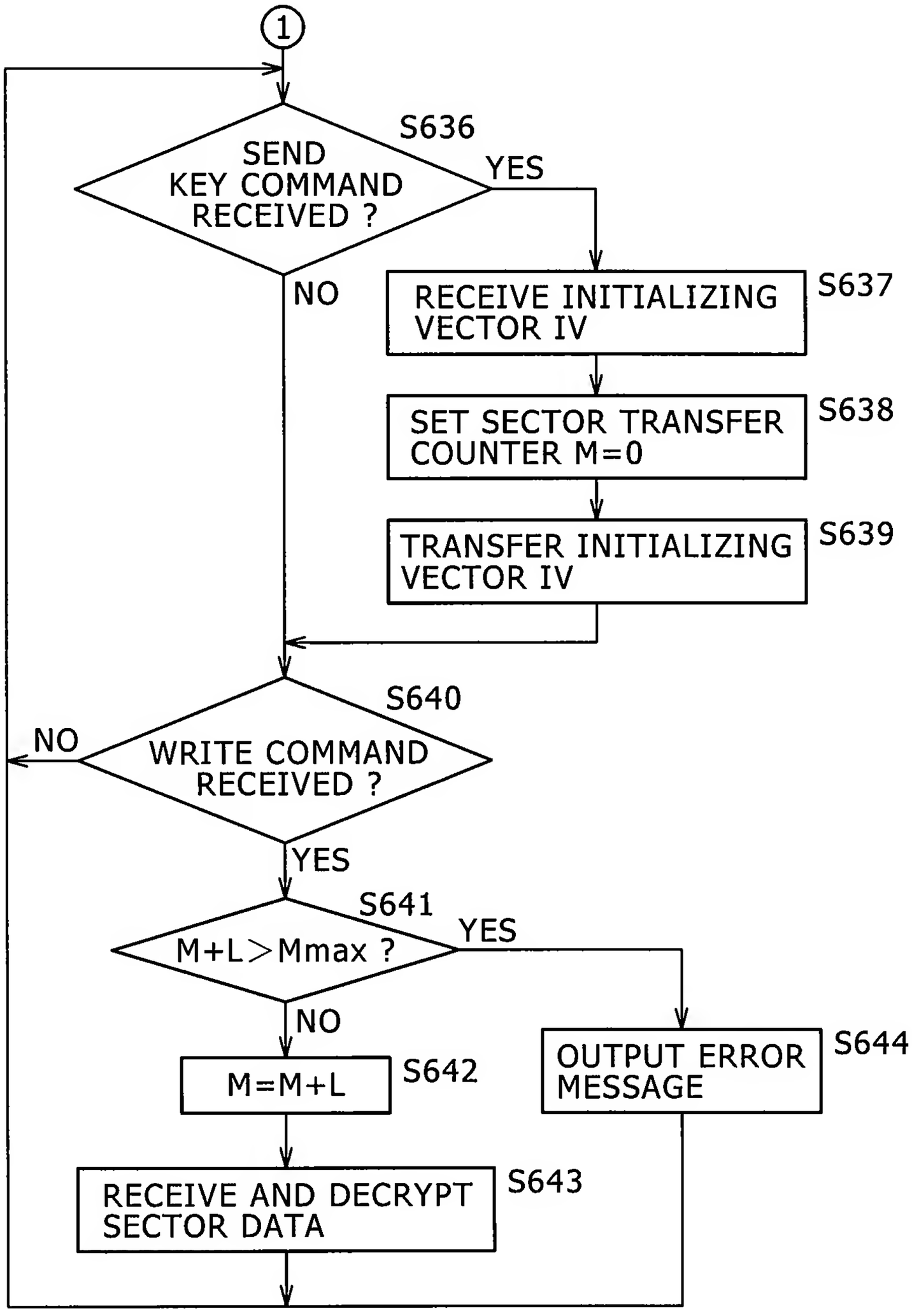

START PROCESSING BY DRIVE UNIT
S631
DISC LOADED ?
NO
YES
S632
APPLICATION STARTED ?
NO
YES
HAVE DRIVE AND HOST AUTHENTICATE ONE ANOTHER AND GENERATE SESSION KET Ks EACH
S633
S634
KEY GENERATION COMPLETED ?
NO
YES
SET SECTOR TRANSFER COUNTER M=Mmax
S635
1

FIG.27


1
S636
SEND KEY COMMAND RECEIVED ?
YES
NO
S637
RECEIVE INITIALIZING VECTOR IV
S638
SET SECTOR TRANSFER COUNTER M=0
S639
TRANSFER INITIALIZING VECTOR IV
S640
WRITE COMMAND RECEIVED ?
NO
YES
S641
M+L>Mmax ?
YES
NO
S642
M=M+L
S643
RECEIVE AND DECRYPT SECTOR DATA
S644
OUTPUT ERROR MESSAGE